SOPHOS

SafeGuard® LAN Crypt 3.71 Client

Benutzerhandbuch

Stand: Dezember 2010

Inhalt

1 Überblick 2

2 Installation 13

3 Deinstallation 17

4 Terminal Server 18

5 SafeGuard LAN Crypt Benutzeranwendung 20

6 Rechtlicher Hinweis 41

7 Technischer Support 42

1 Überblick

1.1 Was ist SafeGuard LAN Crypt?

SafeGuard LAN Crypt ist ein Produkt zur transparenten Dateiverschlüsselung. Es wurde entwickelt, um den vertraulichen Austausch von Daten zwischen Benutzern innerhalb von Berechtigungsgruppen in großen Organisationen zu ermöglichen.

Im Gegensatz zu anderen Verschlüsselungsprodukten arbeitet SafeGuard LAN Crypt ohne Benutzerinteraktion. Es unterstützt die Rolle eines Security Officers, der für Dateien, die mit SafeGuard LAN Crypt verschlüsselt sind, auch die Zugriffsrechte des Systemadministrators einschränken kann. Ein Master Security Officer kann Rechte zur Administration von SafeGuard LAN Crypt auch delegieren und so eine Administrationshierarchie schaffen, die der Organisationsform jedes Unternehmens gerecht wird.

Jedes Mal, wenn ein Benutzer eine Datei in ein verschlüsseltes Verzeichnis verschiebt, wird die Datei auf dem Computer dieses Benutzers verschlüsselt. Wenn ein anderer Benutzer aus derselben Berechtigungsgruppe die Datei aus dem Verzeichnis liest, wird sie in verschlüsselter Form übertragen. Erst auf dem Zielcomputer wird die Datei entschlüsselt, eventuell verändert und erneut verschlüsselt, bevor sie wieder zurück in das verschlüsselte Verzeichnis gestellt wird.

Verschlüsselte Dateien sind nicht an einen einzelnen Benutzer gebunden. Alle Benutzer, die den notwendigen Schlüssel besitzen, können auf die verschlüsselte Datei zugreifen. Dies erlaubt Security Officers das Erzeugen von logischen Benutzergruppen, die gemeinsam auf verschlüsselte Dateien zugreifen können. Dieser Vorgang kann mit einer Art Schlüsselbund, wie er im täglichen Leben verwendet wird, verglichen werden: SafeGuard LAN Crypt stattet Benutzer und Benutzergruppen mit einem Schlüsselbund aus, dessen Schlüssel für verschiedene Türen oder Safes verwendet werden können.

Nicht berechtigte Benutzer können eventuell auf diese verschlüsselten Dateien zugreifen (nur von Arbeitsstationen ohne SafeGuard LAN Crypt), können die Daten aber ohne die entsprechende SafeGuard LAN Crypt Berechtigung nicht lesen.

Auf diese Weise bleibt die Datei immer geschützt, auch wenn im Dateisystem selbst kein Zugriffsschutz definiert ist, das Netzwerk angegriffen wird oder die Mitarbeiter sich nicht an die Sicherheitsrichtlinien der Organisation halten.

SafeGuard LAN Crypt sollte das Produkt Ihrer Wahl sein, wenn es darum geht, geistiges Eigentum in Dateiform vor unberechtigtem Zugriff in einem LAN, auf einem File-Server, auf der lokalen Festplatte oder auf mobilen Datenträgern zu schützen.

1.2 Schutz von Daten durch SafeGuard LAN Crypt

SafeGuard LAN Crypt garantiert, dass sensible Dateien auf File-Servern und Arbeitsstationen verschlüsselt gespeichert werden können. Ebenso erfolgt die Übertragung in Netzwerken (LAN oder WAN) geschützt, da Ver- und Entschlüsselung im Hauptspeicher der Arbeitsstation des Benutzers durchgeführt werden. Auf dem File-Server selbst muss keine spezielle Sicherheitssoftware installiert werden.

Die Richtliniendateien enthalten alle Regeln, Zugriffsrechte und Schlüssel, die für die transparente Verschlüsselung benötigt werden. Damit ein Benutzer auf seiner Arbeitsstation Daten mit SafeGuard LAN Crypt ver- und entschlüsseln kann, muss er in der Lage sein, auf die Richtliniendatei zuzugreifen. Die Richtliniendatei ist durch ein Zertifikat vor unberechtigtem Zugriff gesichert. Um Zugriff zu erhalten, muss ein Benutzer über den privaten Schlüssel des passenden Zertifikats verfügen.

Auf den Arbeitsstationen laufen alle Ver- und Entschlüsselungen transparent und weitgehend ohne die Notwendigkeit von Benutzerinteraktionen ab.

SafeGuard LAN Crypt ermöglicht die Einteilung der Benutzer in verschiedene Berechtigungsgruppen durch die Definition unterschiedlicher Rechte auf Verzeichnis- und Dateiebene. Die Sammlung dieser Rechte ergibt ein Verschlüsselungsprofil für den Benutzer. Durch den Besitz des zum Zertifikat gehörenden privaten Schlüssels hat der Benutzer Zugriff auf seine Richtliniendatei, in der das Verschlüsselungsprofil gespeichert ist.

Alle SafeGuard LAN Crypt Benutzer, die in ihrer Richtliniendatei dasselbe Verschlüsselungsprofil gespeichert haben, sind Mitglieder einer Berechtigungsgruppe. Die Benutzer müssen sich dazu weder um die Verschlüsselung noch um den Schlüsselaustausch kümmern. Sie müssen nur in der Lage sein, auf die Richtliniendateien zuzugreifen. Ist diese Voraussetzung erfüllt, werden die Dateien der Benutzer transparent ver- bzw. entschlüsselt, sobald sie geöffnet bzw. geschlossen werden.

Durch die Verteilung der Verschlüsselungsprofile über Richtliniendateien können alle Organisationsformen abgebildet werden: von einem zentralen LAN-Modell, in dem die Benutzer zentral administriert werden, bis zu einem verteilten Modell, in dem Benutzer Notebooks einsetzen.

SafeGuard LAN Crypt Administration und Windows Administration

Die Verwaltung der Verschlüsselungsprofile und die Konfiguration von SafeGuard LAN Crypt erfolgt auf einem eigenen Administrationsrechner. Um eine klare Unterscheidung zwischen der Windows Administration und der Administration von SafeGuard LAN Crypt zu erreichen, wird die Rolle eines Security Officers eingerichtet. Der Security Officer legt durch die Definition der Verschlüsselungsprofile in Richtliniendateien fest, welche verschlüsselten Daten in welchen Verzeichnissen abzulegen sind und wer auf diese Daten Zugriff hat. Nach der Erzeugung der Richtliniendateien auf dem Administrationsrechner müssen diese an die Benutzer verteilt werden.

Zur Administration von SafeGuard LAN Crypt wird ein Windows-Standardmechanismus, die Microsoft Management Konsole (MMC), verwendet. Die Benutzeroberfläche der SafeGuard LAN Crypt Administration besteht aus Snap-Ins für die MMC. Die SafeGuard LAN Crypt Administration speichert die meisten administrierbaren Objekte (Benutzerdaten, Schlüssel, Verschlüsselungspfade, etc.) in einer eigenen Datenbank.

Die Verwendung des Datenbankkonzepts anstelle von ausschließlich Windows-Mechanismen (z. B. Active Directory) hat vor allem zwei Vorteile:

- Systemadministration und Security-Administration können streng getrennt werden. Die Verwendung einer eigenen Datenbank macht SafeGuard LAN Crypt unabhängig von der Systemadministration. Die Schlüssel in der SafeGuard LAN Crypt Administrationsdatenbank sind verschlüsselt und dadurch vor unberechtigtem Zugriff geschützt. Zusätzlich verhindert die Datenbank, dass unbeabsichtigt Änderungen vorgenommen werden (z. B. dass ein Systemadministrator ein benötigtes Sicherheitsobjekt löscht).

- Andererseits ist es oft nicht erwünscht, dass Personen, die keine Systemadministratoren sind, die Systemkonfiguration ändern können. Es liegt auf der Hand, dass es problematisch ist, Schreibrechte bei der Systemadministration zu delegieren. Auch aus dieser Sicht ist es sehr sinnvoll, die SafeGuard LAN Crypt spezifischen Daten in einer separaten Datenbank zu speichern.

Um den bestmöglichen Schutz zu bieten, sind die SafeGuard LAN Crypt Funktionen wiederum in zwei Bereiche gegliedert:

- **SafeGuard LAN Crypt Benutzerfunktionen**
  Die SafeGuard LAN Crypt Benutzerfunktionen enthalten die Ver-/Entschlüsselungsinformationen der Daten, die zur täglichen Arbeit mit SafeGuard LAN Crypt notwendig sind. Sobald ein Benutzer auf die Schlüsselinformationen zugreifen kann, werden die Dateien transparent ver- bzw. entschlüsselt. Es ist ansonsten kein Benutzereingriff mehr notwendig.
  Zusätzlich bietet SafeGuard LAN Crypt einige Anzeigefunktionen, die es dem Benutzer ermöglichen, sich “seine” Verschlüsselungsvorschriften anzeigen zu lassen.

- **SafeGuard LAN Crypt Security Officer Funktionen**
  Die SafeGuard LAN Crypt Administration bietet Funktionen, die einem Security Officer vorbehalten sind.
  Verschlüsselungsprofile können nur dann administriert werden, wenn man im Besitz des Security Officer-Zertifikats ist. Nur dann ist es möglich, Verschlüsselungsprofile zu erzeugen und bestehende zu verwalten.
  Die SafeGuard LAN Crypt Administration kann getrennt vom Benutzerprogramm installiert werden, da nur ein Security Officer Zugriff darauf haben sollte.

1.3 Transparente Verschlüsselung

Transparente Verschlüsselung bedeutet für den Benutzer, dass alle verschlüsselt gespeicherten Daten (sei es in verschlüsselten Verzeichnissen oder Laufwerken) automatisch im Hauptspeicher entschlüsselt werden, sobald sie in einem Programm geöffnet werden. Beim Abspeichern der Datei wird diese automatisch wieder verschlüsselt.

- Alle Dateien, für die eine Verschlüsselungsregel existiert, werden automatisch verschlüsselt.
- Werden Dateien in ein verschlüsseltes Verzeichnis verschoben oder kopiert, werden sie gemäß der für dieses Verzeichnis definierten Verschlüsselungsregel verschlüsselt. Natürlich ist es möglich, verschiedene Verschlüsselungsregeln für verschiedene Dateierweiterungen oder -namen in ein und demselben Verzeichnis festzulegen. Die Verschlüsselung ist nicht von Verzeichnissen abhängig, sondern nur von Verschlüsselungsregeln!
- Beim Umbenennen von verschlüsselten Dateien bleiben diese verschlüsselt (sofern nicht eine andere oder keine Verschlüsselungsregel für den neuen Dateinamen oder die neue Dateierweiterung besteht).
- Kopieren oder verschieben Sie verschlüsselte Dateien an einen Ort, an dem die bisherige Verschlüsselungsregel nicht mehr gilt, werden sie automatisch entschlüsselt.
- Wurde vom Administrator die *Persistente Verschlüsselung* aktiviert, bleiben Dateien auch dann verschlüsselt, wenn sie im Windows Explorer an einen Ort verschoben wurden, für den keine Verschlüsselungsregel gilt. Werden Dateien außerhalb des Windows Explorer kopiert oder verschoben (z. B. Kommandozeile), hat diese Funktion keine Auswirkung und die Dateien werden entschlüsselt.
- Kopieren oder verschieben Sie verschlüsselte Dateien an einen Ort, an dem nicht mehr die bisherige Verschlüsselungsregel gilt, sondern eine andere, werden die betreffenden Dateien zuerst entschlüsselt und danach anhand der neuen Regel wieder verschlüsselt.
- Transparente Verschlüsselung betrifft alle Arbeiten mit Dateien. Der Benutzer bemerkt nichts von den Ver- bzw. Entschlüsselungsvorgängen, da alle Prozesse im Hintergrund ablaufen.

Hinweis: SafeGuard LAN Crypt kann keine Dateien verschlüsseln, für die unter dem NTFS Dateisystem von Windows die NTFS-Komprimierung und die EFS-Verschlüsselung verwendet wird. Der Assistent zur Initialverschlüsselung bietet allerdings die Möglichkeit, wenn für NTFS-komprimierte und/oder EFS-verschlüsselte Dateien eine Verschlüsselungsregel besteht, diese im Rahmen der Initialverschlüsselung zur dekomprimieren bzw. zu entschlüsseln. Die Dateien werden anschließend von SafeGuard LAN Crypt den Verschlüsselungsregeln entsprechend verschlüsselt.
Ob der Benutzer die Möglichkeit hat, NTFS-komprimierte Dateien zu dekomprimieren oder EFS- verschlüsselte Dateien wenn notwendig zu entschlüsseln, wird vom Security Officer festgelegt.

1.3.1 Zugriff auf verschlüsselte Daten

Gibt es in den Verschlüsselungsvorschriften eines Benutzers keinen Schlüssel und keine Verschlüsselungsregel für ein Verzeichnis, darf er nicht auf die verschlüsselten Dateien in diesem Verzeichnis zugreifen. Er darf dort keine verschlüsselte Datei lesen, kopieren, verschieben, umbenennen etc.

Verfügt der Benutzer über den Schlüssel, mit dem die Dateien verschlüsselt sind, kann er, auch wenn in seinen Verschlüsselungsvorschriften keine Verschlüsselungsregel auf diese Dateien verweist, diese Dateien öffnen.

Hinweis: Beim Abspeichern von Dateien, die „nur“ mit dem vorhandenen Schlüssel (keine Verschlüsselungsregel für diese Dateien) geöffnet wurden, kann es dazu kommen, dass diese unverschlüsselt angelegt werden. Dies ist bei Programmen der Fall, die beim Speichern eine temporäre Datei anlegen, die Quelldatei dann löschen und anschließend die temporäre Datei umbenennen. Da für die neu angelegte Datei keine Verschlüsselungsregel existiert, wird sie unverschlüsselt angelegt. Um das zu verhindern muss ein solches Programm als "Programm mit speziellem Speicherverhalten" eingetragen werden (siehe *Programme mit speziellem Speicherverhalten* auf Seite 25).

1.3.2 Verzeichnisse umbenennen oder verschieben

SafeGuard LAN Crypt führt aus Performance-Gründen beim Verschieben ganzer Verzeichnisse innerhalb eines Laufwerks über den Windows Explorer keine Änderung des Verschlüsselungsstatus durch. Das bedeutet, dass es beim Verschieben eines Verzeichnisses zu keiner Ver-, Ent- bzw. Umschlüsselung kommt.

Waren die Dateien in diesen Verzeichnissen verschlüsselt, bleiben sie unter dem neuen Verzeichnisnamen bzw. am neuen Speicherort verschlüsselt. Besitzt der Benutzer den entsprechenden Schlüssel, kann er wie gewohnt mit diesen Dateien arbeiten.

Anders ist das Verhalten beim Verschieben von Verzeichnissen und Dateien auf eine andere Partition oder auf USB-Speichermedien, für die keine Verschlüsselungsregel eingerichtet wurde. Ist die *Persistente Verschlüsselung* nicht aktiviert, werden die Dateien wie bisher entschlüsselt, wenn sie auf derartige Medien verschoben werden. Hat der Administrator dagegen die Funktion *Persistente Verschlüsselung* aktiviert, bleiben die Dateien auch in diesem Fall verschlüsselt.

Werden Dateien außerhalb des Windows Explorer kopiert oder verschoben (z. B. Kommandozeile), hat die *Persistente Verschlüsselung* keine Auswirkung und die Dateien werden entschlüsselt.

Sicheres Verschieben

SafeGuard LAN Crypt bietet eine eigene Funktion für das Verschieben von Dateien und Verzeichnissen. Beim Verschieben durch SafeGuard LAN Crypt werden die Dateien auch am neuen Speicherort entsprechend den geltenden Verschlüsselungsregeln ver-, ent- bzw. umgeschlüsselt. Die Quelldateien werden nach dem Verschieben sicher gelöscht.

Diese Funktion steht über den Eintrag **Sicheres Verschieben** im Windows Explorer Kontextmenü von SafeGuard LAN Crypt zur Verfügung. Über einen Dialog kann dann ausgewählt werden, wohin die Dateien verschoben werden sollen.

1.3.3 Explizite Entschlüsselung von Dateien

Wenn eine Datei entschlüsselt werden soll, muss sie nur in ein Verzeichnis kopiert oder verschoben werden, für das keine Verschlüsselungsregel existiert. Dabei wird sie automatisch entschlüsselt.

Dies gilt allerdings nur unter der Bedingung, dass

- ein entsprechendes Verschlüsselungsprofil geladen ist,
- Sie über den richtigen Schlüssel verfügen,
- im aktiven Verschlüsselungsprofil keine Verschlüsselungsregel für den neuen Ablageort existiert,
- und die *Persistente Verschlüsselung* nicht aktiviert ist.

Hinweis: Die Verschlüsselung durch SafeGuard LAN Crypt funktioniert auch mit Offline Foldern von Windows. Allerdings können hierbei in Verbindung mit Virenscannern unter Umständen Probleme auftreten. Genauere Informationen zu bekannten Problemen mit Virenscannern enthält die Readme-Datei zum SafeGuard LAN Crypt Client.

1.3.4 Löschen verschlüsselter Dateien - Windows Papierkorb

Wenn Ihr Verschlüsselungsprofil geladen ist, können Sie jede verschlüsselte Datei löschen, für die Sie einen Schlüssel besitzen.

Hinweis: Eigentlich handelt es sich beim Löschen von Dateien um ein Verschieben der Dateien in den Windows Papierkorb. Um den höchsten Sicherheitsstandard zu gewährleisten, bleiben die SafeGuard LAN Crypt verschlüsselten Dateien natürlich auch im Papierkorb verschlüsselt. Um diese Dateien endgültig zu löschen, muss der Schlüssel, der zur Verschlüsselung der Dateien verwendet wurde, vorhanden sein. Ist der Schlüssel nicht vorhanden, wird eine Fehlermeldung ausgegeben, und Sie können die betreffenden Dateien nicht von Ihrem System entfernen.

Es können Situationen auftreten, in denen Verschlüsselungsregeln geändert wurden, nachdem eine Datei in den Papierkorb verschoben wurde. In diesem Fall muss der alte Schlüssel verfügbar sein, damit diese Datei endgültig gelöscht werden kann.

1.3.5 Von einer Verschlüsselung ausgenommene Dateien und Verzeichnisse

Folgende Dateien und Verzeichnisse sind von einer Verschlüsselung automatisch ausgenommen (auch wenn für sie eine Verschlüsselungsregel definiert wurde):

- Dateien im Installationsverzeichnis von SafeGuard LAN Crypt,
- Dateien im Installationsverzeichnis von Windows.
- Local Cache

1.3.6 SafeGuard LAN Crypt und SafeGuard Enterprise

Diese Version von SafeGuard LAN Crypt und SafeGuard Enterprise Version 5.35.4 oder höher können gleichzeitig auf einem Computer verwendet werden. Zum Beispiel können alle Dateien auf Wechselmedien mit SafeGuard Enterprise Data Exchange verschlüsselt werden während alle Dateien auf Netzwerklaufwerken mit SafeGuard LAN Crypt verschlüsselt sind.

SafeGuard LAN Crypt zeigt im Dialog *Client Status* alle auf dem System geltenden Verschlüsselungsregeln an. Generell gilt, dass SafeGuard Enterprise Data Exchange Regeln vor jenen von SafeGuard LAN Crypt angewendet werden. Die Priorisierung kann jedoch geändert werden.

Umverschlüsselung von mit SafeGuard Enterprise Data Exchange verschlüsselten Daten

Der Assistent zur Initialverschlüsselung ermöglicht das Umschlüsseln von mit SafeGuard Enterprise Data Exchange verschlüsselten Daten für die keine SafeGuard Enterprise Verschlüsselungsregel mehr gilt. Solche Dateien liegen zum Beispiel vor, wenn die SafeGuard Enterprise Verschlüsselungsregel aufgehoben wurde, die Dateien aber nicht explizit entschlüsselt wurden. In diesem Fall, kann im Assistenten zur Initialverschlüsselung die Option **Dateien entsprechend den Regeln umschlüsseln** ausgewählt werden, wodurch diese Dateien den SafeGuard LAN Crypt Verschlüsselungsregeln entsprechend umgeschlüsselt werden.

1.3.7 Laden der Richtliniendatei

Standardverhalten von SafeGuard LAN Crypt

Wenn sich ein Benutzer an Windows anmeldet, wird zuerst sein (zwischen)gespeichertes Benutzerprofil geladen. Danach überprüft SafeGuard LAN Crypt, ob es eine neue Richtliniendatei für den Benutzer gibt, indem es eine Verbindung zum festgelegten Speicherort

für Richtliniendateien (Netzwerklaufwerk) aufbaut. Wird dort einen neuere Richtliniendatei gefunden, wird das zwischengespeicherte Benutzerprofil aktualisiert.

Diese Vorgehensweise hat den Vorteil, dass der Benutzer bereits mit verschlüsselten Daten arbeiten kann, während SafeGuard LAN Crypt überprüft, ob es eine neuere Version der Richtliniendatei gibt.

Ist das Netzwerklaufwerk nicht erreichbar, arbeitet der Benutzer solange mit dem zwischengespeicherten Benutzerprofil, bis dieses aktualisiert werden kann.

Hinweis: SafeGuard LAN Crypt verifiziert die Zertifikate des Benutzers und des (Master) Security Officers. Wenn das Zertifikat einen „CRL Distribution Point" enthält und keine gültige CRL im System vorhanden ist, versucht Windows die CRL von der angegebene Adresse zu importieren. Ist eine Firewall installiert, kann es sein, dass eine Meldung angezeigt wird, dass ein Programm (loadprof.exe) versucht eine Verbindung zum Internet aufzubauen. In manchen Fällen kann auch das Laden des Benutzerprofils diese Meldung auslösen.

Durch Security Officers festgelegtes Verhalten

Ein Security Officer kann das Standardverhalten durch zentrale Einstellungen beeinflussen. Er kann festlegen, wie lange die zwischengespeicherte Richtlinie auf den Client-Computern gültig ist und in welchen Intervallen die Richtliniendatei aktualisiert wird. Die Einstellungen des Security Officers werden im Dialog *Client Status* auf dem Reiter *Profil* angezeigt (siehe *Der Dialog Clientstatus* auf Seite 24).

Innerhalb des angegebenen Zeitraums ist die Richtliniendatei auf dem Client gültig und der Benutzer hat Zugriff auf verschlüsselte Daten, auch wenn keine Verbindung zum Speicherort der Richtliniendatei besteht.

Läuft die angegebene Dauer ab, versucht SafeGuard LAN Crypt noch einmal, die Richtliniendatei vom Netzwerklaufwerk zu laden, um sie zu aktualisieren. Ist dies nicht möglich, wird die Richtliniendatei entladen. Der Benutzer hat keinen Zugriff mehr auf verschlüsselte Daten. Erst wenn wieder eine gültige Richtliniendatei zur Verfügung steht (z. B. bei der nächsten Anmeldung mit einer Verbindung zum Speicherort der Richtliniendateien für die Clients), wird die Richtliniendatei aktualisiert und geladen. Der Benutzer hat wieder Zugriff auf verschlüsselte Daten. Der Zähler für die Dauer der Zwischenspeicherung wird zurückgesetzt.

Die Angabe der Dauer der Zwischenspeicherung kann einerseits sicherstellen, dass die Client-Computer in regelmäßigen Intervallen mit aktuellen Richtliniendateien versorgt werden und die Benutzer immer aktuelle Richtlinien verwenden, andererseits kann durch die Beschränkung der Gültigkeitsdauer verhindert werden, dass Benutzer mit Richtliniendateien unbeschränkt lange weiterarbeiten können. Denn solange die Richtliniendateien durch eine Verbindung zum Speicherort für Richtliniendateien nicht aktualisiert werden, kann ein Benutzer mit einer zwischengespeicherten Version der Richtliniendatei unbeschränkt lange arbeiten, wenn diese Einstellung auf *nicht konfiguriert* gesetzt ist.

In folgenden Fällen wird der Zähler für die erlaubte Dauer der Zwischenspeicherung zurückgesetzt:

- Der Speicherort der Richtliniendateien ist erreichbar, es wurde eine gültige Richtliniendatei auf den Client übertragen (z. B. bei der Anmeldung des Benutzers, oder ausgelöst durch ein eingestelltes Aktualisierungsintervall), diese ist aber nicht neuer als die bestehende.
- Eine neue Richtliniendatei ist verfügbar und wurde erfolgreich geladen.

In folgenden Fällen wird der Zähler für die erlaubte Dauer der Zwischenspeicherung NICHT zurückgesetzt:

- Der Client-Computer versucht, eine neue Richtliniendatei zu erhalten, der Speicherort der Richtliniendateien ist aber nicht erreichbar.
- Eine neue Richtliniendatei wurde übertragen, konnte aber aufgrund eines Fehlers nicht geladen werden.
- Es ist eine neue Richtliniendatei verfügbar, sie verlangt aber ein neues Zertifikat. Der Benutzer besitzt dieses Zertifikat nicht oder kann es nicht laden.

Schlägt die Aktualisierung der Richtliniendatei fehl, wird auf dem Client-Computer der Ablaufzeitpunkt der zwischengespeicherten Richtliniendatei in Form einer Balloon-Hilfe angezeigt. Der Benutzer kann dann eine manuelle Aktualisierung über das SafeGuard LAN Crypt System-Tray-Icon anstoßen (siehe *Verschlüsselungsregeln laden/Verschlüsselungsregeln aktualisieren* auf Seite 22).

Keine Zwischenspeicherung der Richtliniendatei

Ein Security Officer kann auch festlegen, dass die Richtliniendatei nicht zwischengespeichert wird. Das bedeutet, dass der Benutzer sein Benutzerprofil bei der Anmeldung erhält, wenn der Speicherort der Richtliniendatei erreichbar ist. Ist dieser nicht erreichbar oder tritt ein Fehler beim Laden des Profils auf, kann der Benutzer nicht auf verschlüsselte Daten zugreifen.

Clients ab Version 3.12

Diese Funktionalität steht für ältere Client-Versionen nicht zur Verfügung. Clients ab der Version 3.12 können jedoch mit Version 3.60 der SafeGuard LAN Crypt Administration betrieben werden. Diese Clients verhalten sich beim Laden der Richtliniendateien wie folgt:
Es wird immer versucht, die Richtliniendatei aus dem angegebenen Speicherort zu laden. Ist dieser nicht erreichbar, wird eine zwischengespeicherte Version der Richtliniendatei geladen. Diese zwischengespeicherte Richtliniendatei hat kein Ablaufdatum und wird erst aktualisiert, wenn eine neuere Version erfolgreich geladen wurde. Es kann auch kein Aktualisierungsintervall für die Richtlinien festgelegt werden. Zwischengespeicherte Richtliniendateien behalten ihre Gültigkeit, bis der Speicherort erreichbar ist und sie durch eine von dort neu geladene Datei ersetzt werden können.

1.4 Systemanforderungen

1.4.1 Plattformen

SafeGuard LAN Crypt Client ist für folgende Betriebssysteme verfügbar:

- Windows XP SP2 32bit
- Windows XP SP3 32bit
- Windows Vista Ultimate SP1 32bit
- Windows Vista Enterprise SP1 32bit
- Windows Vista Business SP1 32bit
- Windows Vista Ultimate SP2 32bit
- Windows Vista Enterprise SP2 32bit
- Windows Vista Business SP2 32bit
- Windows 7 Professional 32bit
- Windows 7 Enterprise 32bit
- Windows 7 Ultimate 32bit
- Windows 7 Professional 64bit
- Windows 7 Enterprise 64bit
- Windows 7 Ultimate 64bit

1.4.2 Firewall

Nachdem sich ein Benutzer angemeldet hat, versucht SafeGuard LAN Crypt das Benutzerprofil zu laden. Dabei werden die Zertifikate von Benutzer und (Master) Security Officer überprüft. Enthält ein Zertifikat einen "CRL Distribution Point“ und es ist keine gültige CRL auf dem System verfügbar, versucht Windows eine CRL von der angegebenen Adresse zu importieren. Ist eine Firewall aktiv, wird unter Umständen eine Meldung angezeigt, dass ein Programm (loadprof.exe) versucht, eine Verbindung zum Internet herzustellen.

1.5 SafeGuard LAN Crypt und SafeGuard Enterprise

- SafeGuard LAN Crypt 3.7x und SafeGuard Enterprise 5.35.4 und höher können ohne Einschränkungen auf einem Computer installiert werden und sind in vollem Umfang kompatibel.
- SafeGuard LAN Crypt Versionen unter 3.7x und SafeGuard Enterprise 5.4x können nicht gleichzeitig auf einem Computer installiert werden.
  Wenn Sie SafeGuard Enterprise 5.4x auf einem Computer installieren möchten, auf dem bereits SafeGuard LAN Crypt 3.6x oder niedriger installiert ist, wird die Installation

abgebrochen und eine entsprechende Fehlermeldung angezeigt.

- SafeGuard LAN Crypt 3.7x und SafeGuard Enterprise Versionen niedriger als 5.35.4 können nicht gemeinsam auf einem Computer installiert werden.
  Wenn Sie SafeGuard LAN Crypt 3.7x auf einem Computer installieren möchten, auf dem bereits SafeGuard Enterprise in einer niedrigeren Version als 5.35.4 installiert ist, wird die Installation abgebrochen und eine entsprechende Fehlermeldung angezeigt.

2 Installation

Hinweis: Die Installation von SafeGuard LAN Crypt ist nur möglich, wenn Sie mit Administratorrechten an das Betriebssystem angemeldet sind.

1. Doppelklicken Sie auf eine **.msi-Datei** im `Install` Verzeichnis der Installations-CD.
   - **sglc_x64.msi** für die Installation auf einem 64bit Betriebssystem **oder**
   - **sglc.msi** für die Installation auf einem 32bit Betriebssystem

   Klicken Sie auf **Weiter**.

2. Der Dialog *Lizenzvertrag* wird angezeigt.
   Bitte aktivieren Sie die Option **Ich akzeptiere den Lizenzvertrag**. Wenn Sie dies nicht tun, ist eine Installation von SafeGuard LAN Crypt nicht möglich! Klicken Sie auf **Weiter.**

3. Der Dialog *Zielordner* wird angezeigt.
   Wählen Sie aus, wo SafeGuard LAN Crypt installiert werden soll.
   Klicken Sie auf **Weiter**.

4. Der Dialog *Installationsart auswählen* wird angezeigt.
   In diesem Dialog können Sie auswählen, welche Komponenten von SafeGuard LAN Crypt installiert werden sollen.

- **Standard:**
  Installation der gebräuchlichsten Anwendungsfunktionen des SafeGuard LAN Crypt Client
- **Vollständig:**
  Komplette Client Installation
- **Anpassen:**
  Die einzelnen Komponenten sind auswählbar.

  Wählen Sie **Anpassen** und klicken Sie auf **Weiter**.

Folgende Komponenten können installiert werden:

- **Client Installation**
  - Explorererweiterungen

    Installiert die SafeGuard LAN Crypt Explorererweiterungen.
    SafeGuard LAN Crypt fügt dem Windows Explorer Einträge hinzu, die die Initialverschlüsselung von Dateien und Verzeichnissen, die explizite Ver- und Entschlüsselung von Dateien und Verzeichnissen und die einfache Kontrolle über den Verschlüsselungsstatus Ihrer Dateien erlauben. Die Einträge erscheinen in den Kontextmenüs von Laufwerken, Verzeichnissen und Dateien. Des Weiteren wird auch dem Windows-*Eigenschaften*-Fenster für Dateien eine Seite *Verschlüsselungsinformationen* hinzugefügt.

  - Benutzerprogramm

    Installiert die SafeGuard LAN Crypt Benutzerapplikation.
    Ein Symbol in der Task-Leiste repräsentiert das SafeGuard LAN Crypt Benutzerprogramm. Es zeigt den Status von SafeGuard LAN Crypt durch ein Schlüsselsymbol an.
    Die Applikation bietet (über die rechte Maustaste) dem Benutzer die folgenden Funktionen:

    - Verschlüsselungsregeln laden / aktualisieren
    - Lösche Verschlüsselungsregeln
    - Verschlüsselung deaktivieren/aktivieren
    - Profil anzeigen
    - Clientstatus
    - Initialverschlüsselung
    - Schließen
    - Info

  - Client API

    API zur Automatisierung von Aufgaben am SafeGuard LAN Crypt Client.

5. Wählen Sie aus, welche Komponenten installiert werden sollen und klicken Sie auf **Weiter**.
6. Nachdem Sie Ihre Angaben noch einmal prüfen können, wird nach Klicken auf **Weiter** die Installation gestartet.
7. Nach erfolgreicher Installation wird ein Dialog angezeigt, in dem Sie durch Klicken auf die Schaltfläche **Fertigstellen** die Installation beenden.

Hinweis: Um alle Einstellungen zu übernehmen, müssen Sie das System neu starten, damit der Treiber geladen wird!

2.1 Installation ohne Benutzerinteraktion

Die Installation ohne Benutzerinteraktion erlaubt die automatische Installation von SafeGuard LAN Crypt auf einer großen Zahl von Rechnern.
Das Verzeichnis `Install` Ihrer Installations-CD enthält die `.msi`-Datei zur Installation der Benutzerkomponenten.

2.1.1 Installierbare Komponenten

Die folgende Liste zeigt alle Komponenten, die Sie installieren können und die Art und Weise, wie sie bei der Installation ohne Benutzerinteraktion angegeben werden müssen.

Die Schlüsselwörter (Courier, fett) geben an, wie die einzelnen Komponenten unter ADDLOCAL= angegeben werden müssen, wenn eine Installation ohne Benutzerinteraktion ausgeführt wird.
Die Bezeichnungen der einzelnen Komponenten sind case-sensitive!

ADDLOCAL=ALL installiert alle verfügbaren Komponenten.

Explorererweiterungen **`- ShellExtensions`**

Benutzerprogramm - **`UserApplication`**

Client API - **`ClientAPI`**

2.1.2 Kommandozeilensyntax

Zum Ausführen einer Installation ohne Benutzerinteraktion muss `msiexec` mit bestimmten Parametern aufgerufen werden.

Unbedingt erforderliche Parameter:
`/I`
Gibt das Installations-Package an, das zu installieren ist.

`/QN`
Installation ohne Benutzerinteraktion.

Name der `.msi`-Datei:
`sglc.msi` für 32bit Betriebssysteme
`sglc_x64.msi` für 64bit Betriebssysteme

Syntax:

```
msiexec /i <Pfad>\sglc.msi | sglc_x64.msi /qn
ADDLOCAL=<Komponente1>,<Komponente2>,...
```

Optionale Parameter:

`/L* <Pfad + Dateiname>`

Protokolliert alle Warnungen und Fehlermeldungen in der unter `<Pfad + Dateiname>` angegebenen Datei.

Beispiel

```
msiexec /i C:\Install\sglc.msi /qn ADDLOCAL=ALL
```

Die Installation von SafeGuard LAN Crypt (32bit) wird ausgeführt. Das Programm wird im Standardverzeichnis (`<Systemlaufwerk>:\ Programme\Sophos`) installiert. Die `.msi`-Datei befindet sich im Verzeichnis **Install** auf Laufwerk C.

3 Deinstallation

Der SafeGuard LAN Crypt Client kann nur deinstalliert werden, wenn Sie mit Administratorrechten an das Betriebssystem angemeldet sind.

Bitte beachten Sie, dass verschlüsselte Dateien nach der Deinstallation nicht mehr entschlüsselt werden können!

Achtung: Installieren Sie den SafeGuard LAN Crypt Client nach einer Deinstallation nicht erneut, ohne dass Sie das System neu starten. Sie müssen den Computer mindestens einmal neu starten bevor Sie SafeGuard LAN Crypt erneut installieren.

4 Terminal Server

Diese Version von SafeGuard LAN Crypt unterstützt Windows Terminal Server und Citrix Terminal Server.

4.1 Systemanforderungen

4.1.1 Plattformen

SafeGuard LAN Crypt Client ist für folgende Betriebssysteme verfügbar:

- Windows Server 2003 R2 SP2 32bit mit Terminal Server Services
- Windows Server 2008 R2 64bit mit Terminal Server Services
- Citrix Presentation Server 4.5 32bit mit Hotfix Rollup Pack 3 auf Windows Server 2003 R2 SP2 32bit
- Citrix XenApp 6 auf Windows Server 2008 R2 64bit

4.1.2 Firewall

Nachdem sich ein Benutzer angemeldet hat, versucht SafeGuard LAN Crypt das Benutzerprofil zu laden. Dabei werden die Zertifikate von Benutzer und (Master) Security Officer überprüft. Enthält ein Zertifikat einen "CRL Distribution Point“ und es ist keine gültige CRL auf dem System verfügbar, versucht Windows eine CRL von der angegebenen Adresse zu importieren. Ist eine Firewall aktiv, wird unter Umständen eine Meldung angezeigt, dass ein Programm (loadprof.exe) versucht, eine Verbindung zum Internet herzustellen.

4.2 Installation

Generell läuft die Installation ab wie für Nicht-Terminal-Server-Umgebungen beschreiben (siehe Kapitel *Installation*). Verwenden Sie zur Installation auf einem Terminal Server das Installationspaket **`sglcts.msi`** oder **`sglcts_x64.msi`**.

Wichtig:

- Verwenden Sie eine lokale Anmelde-Session mit Administrationsrechten wenn Sie SafeGuard LAN Crypt auf einem Terminal Server installieren.
- Wenn Sie den Citrix Presentation Server oder Citrix XenApp verwenden möchten, installieren Sie diesen bitte bevor Sie SafeGuard LAN Crypt installieren.

4.3 Einschränkungen

Citrix

- Verschlüsselung auf Citrix Client Drive Redirection - Laufwerken wird nicht unterstützt.
- Citrix Streamed Applications werden nicht unterstützt.

5 SafeGuard LAN Crypt Benutzeranwendung

Zur täglichen Arbeit mit SafeGuard LAN Crypt ist beinahe keine Benutzerinteraktion notwendig. Der SafeGuard LAN Crypt Client wurde an mehreren Stellen verbessert, damit die Benutzer noch sicherer mit ihren Dateien umgehen können. Der Anwender wird bei der Ver- und Entschlüsselung vom SafeGuard LAN Crypt Client aktiv unterstützt.

5.1 Anmeldung an SafeGuard LAN Crypt

Die Anmeldung an SafeGuard LAN Crypt besteht darin, dass das in einer Richtliniendatei gespeicherte Verschlüsselungsprofil des Benutzers geladen wird. Das Verschlüsselungsprofil kann nur geladen werden, wenn der Benutzer über das richtige Zertifikat verfügt.

Die SafeGuard LAN Crypt Verschlüsselungsprofile werden von einem Security Officer entsprechend der firmenweiten Sicherheitspolitik erstellt und in Richtliniendateien gespeichert. Die Benutzerrechner erhalten bei der Netzwerkanmeldung die Information, wo diese Richtliniendateien gespeichert sind. Diese Einstellungen werden vom Systemadministrator vorgenommen. Der Pfad wird in die Windows Registrierung der Client-Rechner eingetragen. SafeGuard LAN Crypt lädt dann aus diesem Verzeichnis die Richtliniendatei für den angemeldeten Benutzer und überprüft anhand des Zertifikats, ob der Benutzer berechtigt ist, das Profil zu laden.

5.1.1 Anmeldung mit Token

Eine Anmeldung an SafeGuard LAN Crypt ist auch mit Token möglich. Voraussetzung dafür ist, dass der Benutzer einen Token besitzt, auf dem sein SafeGuard LAN Crypt Benutzerzertifikat gespeichert ist. Wird das Benutzerzertifkat auf einem mit dem System verbundenen Token gefunden, wird die Anmeldung durchgeführt.

Werden Token zur Anmeldung verwendet, kann es vorkommen, dass SafeGuard LAN Crypt eine Richtliniendatei zu laden versucht, bevor der Token vom Betriebssystem korrekt identifiziert wurde.

In diesem Fall wird eine Meldung angezeigt, dass das Benutzerzertifikat nicht gefunden wurde, obwohl der Token bereits mit dem System verbunden ist.

Der Benutzer muss in diesem Fall die Richtliniendatei manuell laden (Benutzerprogramm in der Task-Leiste > Verschlüsselungsregeln laden). Dadurch wird der Token korrekt identifiziert und die Anmeldung wird durchgeführt.

5.2 Zertifikate

Damit der Benutzer Zugriff auf sein Verschlüsselungsprofil hat, muss das entsprechende Zertifikat auf seinem Computer vorhanden sein. Die Zertifikate müssen den Benutzern vom Security Officer zur Verfügung gestellt werden und von jedem Benutzer importiert werden.

Wurde dies vor der ersten Anmeldung an SafeGuard LAN Crypt durchgeführt, läuft der beschriebene Vorgang vollautomatisch ab.

SafeGuard LAN Crypt bietet die Möglichkeit, die Zertifikate beim ersten Laden der Benutzerprofile automatisch zu importieren. In diesem Fall wird das System vom Security Officer so konfiguriert, dass SafeGuard LAN Crypt bei der ersten Anmeldung auch eine Zertifikatsdatei findet und dann den Importvorgang automatisch startet. Der Benutzer wird einmal aufgefordert, die PIN für den Import der PKCS#12 Schlüsseldatei einzugeben.

Hinweis: Die PIN für den automatischen Import der Zertifikate muss den Benutzern vom Security Administrator mitgeteilt werden.

Das Zertifikat wird bei jedem Laden des Verschlüsselungsprofils geprüft. Wird ein gültiges Zertifikat gefunden, ist der Benutzer an SafeGuard LAN Crypt angemeldet. Ist kein gültiges Zertifikat vorhanden, kann der Benutzer nicht mit den verschlüsselten Daten arbeiten.

Hinweis: Wenn die Anmeldung an SafeGuard LAN Crypt fehlschlägt, erhält der Benutzer eine Fehlermeldung mit einem Hinweis dazu, warum die Anmeldung nicht möglich war. Für eine Auflistung der verschiedenen Fehlermeldungen siehe *Anhang: Fehlermeldungen beim Laden des Profils* auf Seite 39.

Die spezifischen Verschlüsselungsregeln in den SafeGuard LAN Crypt Verschlüsselungsprofilen ermöglichen dem Benutzer den Zugriff auf verschlüsselte Daten. Die Regeln definieren, welche Dateien in welchen Verzeichnissen mit welchem Schlüssel zu verschlüsseln sind. Sobald das Verschlüsselungsprofil eines Benutzers geladen ist, findet die Ver- und Entschlüsselung der Daten transparent im Hintergrund statt, ohne dass der Benutzer davon etwas bemerkt.

Hinweis: CA Zertifikate werden nur dann als korrekt akzeptiert, wenn sie unter „Trusted Root Certification Authorities“ liegen. Die SafeGuard LAN Crypt Software importiert aber CA Zertifikate, die in PKCS#12 Schlüsseldateien enthalten sein können, gemeinsam mit den Benutzerzertifikaten in den Ordner „Personal - Certificates“. Um Fehlermeldungen zu vermeiden, müssen die CA Zeritfikate manuell nach „Trusted Root Certification Authorities“ verschoben werden.

5.3 Benutzerprogramm

Ein Symbol in der Task-Leiste zeigt den Status von SafeGuard LAN Crypt durch ein Schlüsselsymbol an:

- **Grün bedeutet:**
  Verschlüsselungsregeln geladen, transparente Verschlüsselung aktiviert.
- **Gelb bedeutet:**
  Verschlüsselungsregeln geladen, transparente Verschlüsselung deaktiviert.
- **Rot bedeutet:**
  Kein Profil geladen!

Die Applikation bietet (über die rechte Maustaste) dem Benutzer die folgenden Funktionen:

- Verschlüsselungsregeln laden/Verschlüsselungsregeln aktualisieren
- Lösche Verschlüsselungsregeln
- Verschlüsselung deaktivieren/aktivieren
- Profil anzeigen
- Clientstatus
- Initialverschlüsselung
- Schließen
- Info

5.3.1 Benutzermenü

Ein Rechtsklick auf das SafeGuard LAN Crypt Symbol in der Windows Task-Leiste öffnet das Benutzermenü. Dieses Symbol verändert sich entsprechend dem momentanen Status von SafeGuard LAN Crypt.

Hinweis: Welche Menüeinträge tatsächlich sichtbar sind, ist von der Konfiguration des SafeGuard LAN Crypt Clients abhängig. Diese wird vom Security Officer zentral festgelegt.

Das SafeGuard LAN Crypt Benutzermenü enthält folgende Einträge:

- **Verschlüsselungsregeln laden/Verschlüsselungsregeln aktualisieren**
  Mit diesem Befehl wird das aktuell gültige Verschlüsselungsprofil geladen. Wenn z. B. im laufenden Betrieb das Verschlüsselungsprofil geändert wurde, muss es mit diesem Befehl aktualisiert werden.

- **Lösche Verschlüsselungsregeln**

  Löscht das Verschlüsselungsprofil. Auf verschlüsselte Daten kann nicht mehr zugegriffen werden. Dies stellt eine Sicherheitsfunktion dar, die die verschlüsselten Daten auf dem Rechner vor unbefugtem Zugriff schützt, wenn der Arbeitsplatz kurzfristig verlassen werden muss. Diese Funktion macht nur Sinn, wenn die Verwendung des privaten Schlüssels durch die Eingabe eines Passworts geschützt ist. Ansonsten könnte das Profil durch den Befehl **Lade Verschlüsselungsregeln** einfach wieder geladen werden.

- **Verschlüsselung deaktivieren/aktivieren**

  Deaktiviert bzw. aktiviert die transparente Verschlüsselung. Das Ausschalten der transparenten Verschlüsselung ist von Bedeutung, wenn Dateien verschlüsselt bleiben sollen, die von einem verschlüsselten Verzeichnis an einen Ort kopiert/verschoben werden, für den keine Verschlüsselungsregel existiert. Bei aktivierter Verschlüsselung würden diese Dateien entschlüsselt werden, wenn Sie in diesen Ordner kopiert werden.
  Wenn zum Beispiel eine verschlüsselte Datei an eine E-Mail angehängt wird, würde sie bei aktivierter Verschlüsselung automatisch entschlüsselt werden. Ist die transparente Verschlüsselung deaktiviert, können verschlüsselte Dateien als Anhang von E-Mails versendet werden.

Hinweis: Wenn vom Administrator die Funktion **Persistente Verschlüsselung** aktiviert wurde, bleiben verschlüsselte Dateien auch dann verschlüsselt, wenn sie bei aktivierter Verschlüsselung per Windows Explorer an einen Ort kopiert oder verschoben werden, für den keine Verschlüsselungsregel existiert. Werden Dateien außerhalb des Windows Explorer kopiert oder verschoben (z. B. Kommandozeile), hat diese Funktion keine Auswirkung und die Dateien werden entschlüsselt.

- **Profil anzeigen**

  Zeigt auf zwei Reitern die Verschlüsselungsregeln und die in den Verschlüsselungsinformationen enthaltenen Schlüssel an.
  Der Reiter *Aktive Verschlüsselungsregeln* listet die für den angemeldeten Benutzer gültigen Regeln auf. Der Benutzer kann zudem die Optionen '*Ignorieren Regeln anzeigen*' und '*Ausnahmeregeln anzeigen*' wählen, um auch diese Verschlüsselungsregeln zu sehen.
  Der Reiter *Verfügbare Schlüssel* zeigt alle für den aktuellen Benutzer verfügbaren Schlüssel an.

- **Clientstatus**

  Die Funktion **Clientstatus** liefert auf acht Reitern zahlreiche Informationen zum aktuellen Status des SafeGuard LAN Crypt Clients.

- **Initialverschlüsselung**

  Startet den Assistenten für die Initialverschlüsselung der gewünschten Dateien (siehe *Initialverschlüsselung und explizite Verschlüsselung* auf Seite 25).

- **Schließen**

  Beendet das SafeGuard LAN Crypt Benutzerprogramm.

- **Info**

  Zeigt Informationen zur Version von SafeGuard LAN Crypt an.

Hinweis: Schließen schließt nur das SafeGuard LAN Crypt Benutzerprogramm. SafeGuard LAN Crypt bleibt im aktuellen Status. Dies bedeutet, dass die transparente Ver- und Entschlüsselung weiterhin ausgeführt wird. Das Schließen des Benutzerprogramms alleine schützt Daten nicht vor unberechtigtem Zugriff (z. B. wenn ein Benutzer seine Arbeitsstation verlässt).

5.3.2 Der Dialog Clientstatus

Der Dialog **Clientstatus** lässt sich auch über Start/Programme/Sophos/SafeGuard LAN Crypt/ Clientstatus öffnen. Die Funktion *Clientstatus* liefert auf insgesamt acht Reitern nützliche Informationen, z. B. zu den geladenen Verschlüsselungsregeln:

- **Status**

  Zeigt an, ob das Benutzerprofil geladen ist und ob die Verschlüsselung aktiv ist. Zudem enthält der Reiter detaillierte Informationen zur Richtliniendatei (Erstelldatum, Ersteller etc.).
  Ist das Benutzerprofil nicht geladen, ist auch die Verschlüsselung deaktiviert.
  Die Verschlüsselung kann aber bei geladenem Benutzerprofil (temporär) deaktiviert werden (siehe *Verschlüsselung deaktivieren/aktivieren* auf Seite 23).

- **Einstellungen**

  Gibt Auskunft über die aktuell für den Client wirksamen Einstellungen. Diese Einstellungen werden zentral vom Security Officer festgelegt und betreffen die Verschlüsselung, das System-Tray-Icon und Einstellungen für den Assistenten zur Initialverschlüsselung. Es wird unter anderem angezeigt, ob die Ver- und Entschlüsselung erlaubt ist, ob die persistente Verschlüsselung aktiviert ist und welche Menüeinträge auf dem Client-Computer angezeigt werden.

- **Profil**

  Hier werden vom Security Officer die zentral festgelegten Einstellungen für das Benutzerprofil angezeigt.

- **Zertifikate**

  Zeigt Details zum Benutzerzertifikat (Antragsteller, Seriennummer, Gültigkeit) sowie die für den Client geltenden Regeln für die Zertifikatsüberprüfung.

- **Schlüssel**

  Zeigt Informationen zu allen für das aktuell geladene Profil verfügbaren Schlüssel.

- **Regeln**

  Listet die für den aktuellen Benutzer gültigen Verschlüsselungsregeln. Durch Aktivieren von Kontrollkästchen lassen sich Ausnahmeregeln und Verschlüsselungsregeln anderer SafeGuard Produkte anzeigen.

- **Ausnahmen**

  Gibt Auskunft über unberücksichtigte Anwendungen, Laufwerke und Geräte sowie über die geladenen *Ignorieren Regeln* des aktuellen Benutzers. Die Ausnahmen werden für alle installierten SafeGuard Produkte angezeigt.

  SafeGuard LAN Crypt behandelt standardmäßig bestimmte Anwendungen als „Unberücksichtigte Anwendungen“. Auch diese werden auf diesem Reiter angezeigt.

- **Applikationen**

  Hier werden Programme angezeigt, die von SafeGuard LAN Crypt aufgrund ihres Verhaltens eine besondere Behandlung verlangen.

  Programme mit speziellem Speicherverhalten

  Diese Programme wurden vom Security Officer eingetragen, weil sie aufgrund ihres Verhaltens beim Abspeichern von Dateien ein besonderes Verhalten zeigen und deshalb von SafeGuard LAN Crypt speziell behandelt werden müssen, um problemlos zu funktionieren.

  Antiviren-Software

  Antiviren-Software benötigt zum Scannen von verschlüsselten Dateien den Schlüssel, mit dem diese Dateien verschlüsselt sind.
  Hier vom Security Officer eingetragene Antiviren-Software hat Zugriff auf alle Schlüssel und kann dadurch auch verschlüsselte Dateien prüfen.

- Schaltflächen **Importieren/Exportieren:**

  Mit den beiden Schaltflächen *Importieren* und *Exportieren* lassen sich die SafeGuard LAN Crypt Einstellungen aus einer XML-Datei einlesen oder die aktuellen Client-Settings in ein XML-File exportieren.

5.4 Initialverschlüsselung und explizite Verschlüsselung

Nach der Installation von SafeGuard LAN Crypt muss eine Initialverschlüsselung durchgeführt werden, bei der alle Daten entsprechend dem geladenen Verschlüsselungsprofil verschlüsselt werden.
Die Initialverschlüsselung kann über

- das SafeGuard LAN Crypt System-Tray-Icon
- die SafeGuard LAN Crypt Explorererweiterung (siehe *Explorererweiterungen* auf Seite 34) oder
- das Tool `sglcinit.exe` ausgeführt werden, das auch einen Unattended Modus unterstützt

(siehe *Initialverschlüsselung im Unattended-Modus* auf Seite 31).

Neben der Initialverschlüsselung von ganzen Verzeichnissen ist mit dem Kommandozeilen-Tool `sglcinit.exe` und mit der Explorererweiterung auch die Ver-, Ent- und Umschlüsselung einzelner Dateien möglich.

Die explizite Ver-, Ent- oder Umschlüsselung kann notwendig werden:

- Wenn unverschlüsselte Dateien sich in Verzeichnissen befinden, für die eine Verschlüsselungsregel existiert.
- Wenn verschlüsselte Dateien sich in Verzeichnissen befinden, für die keine Verschlüsselungsregel existiert.
- Wenn Dateien in verschlüsselten Verzeichnissen mit einem falschen Schlüssel verschlüsselt sind.
- Wenn sich die Verschlüsselungsvorschriften im Verschlüsselungsprofil geändert haben.
- Wenn Dateien mit mehreren Schlüsseln verschlüsselt wurden.

5.4.1 Der Assistent zur Initialverschlüsselung

Das Tool für die Initialverschlüsselung `sglcinit.exe` verfügt über einen Assistenten mit einer grafischen Oberfläche. Dieser unterstützt

- das Ver-, Ent- und Umschlüsseln von Dateien
- das Prüfen des Verschlüsselungsstatus von Dateien.

Der Assistent lässt sich auf mehreren Wegen starten:

- über das System-Tray-Icon,
- über Start/Programme/Sophos/SafeGuard LAN Crypt/Initialverschlüsselung
- per Doppelklick auf `sglcinit.exe` im Verzeichnis C:\Programme\Sophos\SafeGuard LAN Crypt\

Hinweis: Die Ver-, Ent- und Umschlüsselung wird immer ausschließlich entsprechend einem Verschlüsselungsprofil vorgenommen. Daher muss ein Verschlüsselungsprofil geladen sein.

5.4.1.1 Initialverschlüsselung durchführen

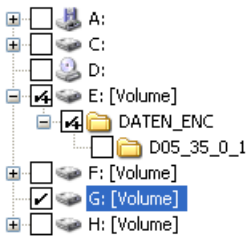
1. Nach dem Starten des Assistenten muss in *Schritt 1/5* die Option **Initialverschlüsselung durchführen** ausgewählt werden.
2. Nach dem Klicken auf **Weiter** kann in *Schritt 2/5* festgelegt werden, wie die Dateien behandelt werden sollen.

- **Dateien entsprechend den Regeln verschlüsseln**
  Wird diese Option ausgewählt, werden die Dateien entsprechend den Regeln im Profil des Benutzers verschlüsselt (Standardeinstellung). Sollten bereits verschlüsselte Dateien gefunden werden, werden diese ignoriert.

- **Dateien entsprechend den Regeln umschlüsseln**
  Wird diese Option aktiviert, werden (auch) Dateien, die mit einem anderen Schlüssel als im Profil festgelegt verschlüsselt sind, entschlüsselt und mit dem korrekten Schlüssel verschlüsselt.
  Voraussetzung dafür ist, dass der Schlüssel, mit dem die Datei(en) bereits verschlüsselt sind, im Profil des Benutzers enthalten ist.
  Diese Option ermöglicht auch das Umschlüsseln von mit SafeGuard Enterprise Data Exchange verschlüsselten Daten, für die keine SafeGuard Enterprise Verschlüsselungsregel mehr gilt. Solche Dateien liegen zum Beispiel vor, wenn die SafeGuard Enterprise Verschlüsselungsregel aufgehoben wurde, die Dateien aber nicht explizit entschlüsselt wurden. Ist diese Option aktiviert, werden solche Dateien den SafeGuard LAN Crypt Verschlüsselungsregeln entsprechend umgeschlüsselt.

Bereits verschlüsselte Daten können entschlüsselt werden, wenn es für sie keine Verschlüsselungsregel (mehr) gibt (siehe *Dateien entschlüsseln* auf Seite 30).

3. Nach dem Klicken auf **Weiter** kann in *Schritt 3 / 5* über eine Verzeichnisbaumstruktur festgelegt werden, welche Ordner verschlüsselt/umgeschlüsselt werden sollen.



Ausgewählte Ordner werden mit einem Häkchen markiert. Ein + Zeichen bei einem Ordner zeigt an, dass sich darin Unterordner befinden, die nicht bearbeitet werden, in denen also keine Verschlüsselung/Umschlüsselung der Dateien durchgeführt wird.
Durch Drücken der Schaltfläche **Profilregeln** werden automatisch alle Verzeichnisse markiert, für die Verschlüsselungsregeln im Profil des Benutzers existieren.
Durch Drücken der Schaltfläche **Erweitert** stehen weitere Einstellungen für die Initialverschlüsselung zur Verfügung:

Hinweis: Welche Einstellung vom Benutzer geändert werden können, ist von der Konfiguration des SafeGuard LAN Crypt Clients abhängig. Diese wird vom Security Officer zentral festgelegt.

- **EFS verschlüsselte Dateien wenn notwendig entschlüsseln**
  Wird diesen Option ausgewählt, entschlüsselt der Assistent EFS verschlüsselte Dateien und verschlüsselt sie anschließend, wenn für sie eine SafeGuard LAN Crypt Verschlüsselungsregel gilt.
  Ist diese Option nicht ausgewählt, werden EFS verschlüsselte Dateien vom Assistenten zur Initialverschlüsselung ignoriert. Sie werden nicht von SafeGuard LAN Crypt umgeschlüsselt, auch wenn für sie eine Verschlüsselungsregel besteht.

- **NTFS komprimierte Dateien wenn notwendig dekomprimieren**
  Wird diese Option ausgewählt, dekomprimiert der Assistent NTFS komprimierte Dateien und verschlüsselt sie anschließend, wenn für sie eine Verschlüsselungsregel gilt.
  Ist diese Option nicht ausgewählt, werden NTFS komprimierte Dateien vom Assistenten zur Initialverschlüsselung ignoriert. Sie werden nicht verschlüsselt, auch wenn für sie eine Verschlüsselungsregel festgelegt wurde.

- **Dateien, die wiederholt mit mehreren Schlüssel verschlüsselt wurden, entschlüsseln/ umschlüsseln**
  Wird diese Option ausgewählt, entschlüsselt der Assistent mehrfach verschlüsselte Dateien und verschlüsselt sie anschließend neu, wenn für sie eine Verschlüsselungsregel gilt. Die Dateien sind dann wieder mit einem Schlüssel verschlüsselt. Diese Option kann nur ausgewählt werden, wenn **Dateien entsprechend den Regeln verschlüsseln** oder **Dateien entsprechend den Regeln umschlüsseln** in Schritt 2/5 ausgewählt wurde. Wurde keine dieser Optionen, gewählt ist diese Option ausgegraut.

- **Nur folgende Dateien einschließen:**
  Werden hier bestimmte Dateitypen angegeben (z. B. .txt, .doc usw.), werden ausschließlich Dateien vom angegebenen Typ vom Assistenten zur Initialverschlüsselung bearbeitet. Diese Einstellung wirkt sich nur auf Dateien aus, für die eine Verschlüsselungsregel existiert. Befinden sich auch noch andere Dateien eines Typs, der nicht hier angegeben wird, in einem Verzeichnis, werden sie bei der Initialverschlüsselung nicht berücksichtigt. Sie werden erst verschlüsselt, wenn sie vom Benutzer geöffnet und wieder abgespeichert werden.
  Zur Angabe mehrerer Dateitypen muss eine durch Strichpunkte getrennte Liste verwendet werden.

4. Nach dem Klicken auf **Weiter** kann in *Schritt 4/5* festgelegt werden, welche Dateien im Bericht über die Initialverschlüsselung enthalten sein sollen.

   Für den Bericht kann der Benutzer zwischen folgenden Optionen wählen:

   - **Nur Fehler berichten**
     Der Statusbericht enthält nur Dateien, bei denen während der Verschlüsselung Fehler aufgetreten sind.

   - **Geänderte Dateien und Fehler berichten**
     Der Statusbericht enthält alle Dateien, die geändert wurden oder bei denen während der Verschlüsselung Fehler aufgetreten sind.

   - **Alle Dateien berichten**
     Der Statusbericht enthält alle Dateien.

5. Nach dem Klicken auf **Weiter** werden in *Schritt 5/5* für jede Datei das **Ergebnis** der Verschlüsselung und der **Schlüsselname** des verwendeten Schlüssels angezeigt.

   Bei Dateien mit fehlgeschlagener Verschlüsselung kann der Benutzer über die Schaltfläche **Wiederholen** sofort einen neuen Verschlüsselungsversuch starten.

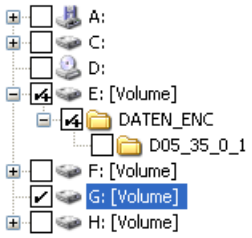
   Die Ergebnisse lassen sich per Mausklick auf die Spaltenüberschrift alphabetisch sortieren. Der Statusbericht kann als XML-Datei an einem gewünschten Ort gespeichert werden (Schaltfläche **Exportieren**). Mithilfe seiner Informationen ist es möglich, die Verschlüsselung der Dateien, bei denen die Verschlüsselung fehlgeschlagen ist, zu einem späteren Zeitpunkt erneut zu versuchen.

   Durch Klicken auf **Fertig** wird der Assistent geschlossen.

5.4.1.2 Verschlüsselungsstatus prüfen

1. Nach dem Starten des Assistenten muss in *Schritt 1/5* die Option **Verschlüsselungsstatus prüfen** ausgewählt werden.

2. Nach dem Klicken auf **Weiter** kann in *Schritt 2/5* über eine Verzeichnisbaumstruktur festgelegt werden, für welche Ordner der Verschlüsselungsstatus geprüft werden soll.



Ausgewählte Ordner werden mit einem Häkchen markiert. Ein + Zeichen bei einem Ordner zeigt an, dass sich darin Unterordner befinden, die nicht bearbeitet werden, in denen also keine Überprüfung des Verschlüsselungsstatus der Dateien durchgeführt wird.

Durch Drücken der Schaltfläche **Profilregeln** werden automatisch alle Verzeichnisse markiert, für die Verschlüsselungsregeln im Profil des Benutzers existieren.

Durch Drücken der Schaltfläche **Erweitert** kann die Prüfung auf bestimmte Dateitypen eingeschränkt werden:

- **Nur folgende Dateien einschließen:**
  Werden hier bestimmte Dateitypen angegeben (z. B. .txt, .doc,...), werden ausschließlich Dateien vom angegebenen Typ geprüft.
  Befinden sich auch noch andere Dateien eines Typs, der nicht hier angegeben wird, in einem Verzeichnis, werden sie nicht berücksichtigt.
  Zur Angabe mehrerer Dateitypen muss eine durch Strichpunkte getrennte Liste verwendet werden.

3. Nach dem Klicken auf **Weiter** werden in *Schritt 3/5* für jede Datei das **Ergebnis** der Prüfung und der **Schlüsselname** des verwendeten Schlüssels angezeigt.

   Die Ergebnisse lassen sich per Mausklick auf die Spaltenüberschrift alphabetisch sortieren. Der Statusbericht kann als XML-Datei an einem gewünschten Ort gespeichert werden (Schaltfläche **Exportieren**).

   Durch Klicken auf **Fertig** wird der Assistent geschlossen.

5.4.1.3 Dateien entschlüsseln

Von SafeGuard LAN Crypt verschlüsselte Daten können entschlüsselt werden, wenn es für sie keine Verschlüsselungsregel (mehr) gibt. Wurde eine erneute Initialverschlüsselung notwendig, weil sich z. B. Verschlüsselungsregeln im Profil des Benutzers geändert haben, können Dateien, für die es nun keine Verschlüsselungsregeln mehr gibt, über diesen Assistenten entschlüsselt werden.

Sollen Dateien entschlüsselt werden, muss in *Schritt 1/5* des Assistenten **Initialverschlüsselung durchführen** und in *Schritt 2/5* unter *Entschlüsselung* die Option **Dateien mit den ausgewählten Schlüsseln entschlüsseln** ausgewählt werden.

Anschließend können die Schlüssel ausgewählt werden. Nur die Dateien, die mit den ausgewählten Schlüsseln verschlüsselt wurden, werden entschlüsselt. Aber nur dann, wenn für sie keine Verschlüsselungsregel mehr gilt.

Hinweis: SafeGuard LAN Crypt entschlüsselt ausschließlich Dateien, für die keine Verschlüsselungsregel gilt.

Beispiel:
Der Assistent zur Initialverschlüsselung wird gestartet, weil Änderungen im Benutzerprofil vorgenommen wurden. Um sicherzustellen, dass nach dem Beenden des Assistenten zur Initialverschlüsselung alle Dateien den gewollten Verschlüsselungsstatus besitzen, kann folgendermaßen vorgegangen werden:

- *Dateien entsprechend den Regeln verschlüsseln* **aktivieren**
  Alle Dateien werden gemäß den neuen Verschlüsselungsregeln verschlüsselt.
- *Dateien entsprechend den Regeln umschlüsseln* **aktivieren**
  Sollten Dateien nach den neuen Regeln mit einem anderen Schlüssel verschlüsselt werden müssen, werden diese umgeschlüsselt.
- *Dateien mit den ausgewählten Schlüsseln entschlüsseln* **aktivieren** und **alle** Schlüssel auswählen.
  Verschlüsselte Dateien, für die es nun keine Verschlüsselungsregel mehr gibt, werden entschlüsselt. SafeGuard LAN Crypt entschlüsselt ausschließlich Dateien, für die es keine Verschlüsselungsregel gibt, darum ist die Auswahl aller Schlüssel völlig unproblematisch.

Alle Dateien besitzen nach dem erfolgreichen Beenden des Assistenten den korrekten Verschlüsselungsstatus.

Das explizite Entschlüsseln von Dateien kann dann wichtig sein, wenn die persistente Verschlüsselung aktiviert ist. In diesem Fall werden Dateien nicht automatisch entschlüsselt, wenn sie aus einem Verzeichnis, für das eine Verschlüsselungsregel gilt, in ein Verzeichnis ohne Verschlüsselungsregel kopiert/verschoben werden.

5.4.2 Initialverschlüsselung im Unattended-Modus

Wenn `sglcinit.exe` im Unattended-Modus ausgeführt werden soll, muss das Tool mit bestimmten Parametern auf einer Kommandozeile aus dem Verzeichnis heraus aufgerufen werden, in dem es sich befindet (z. B. C:\Programme\Sophos\SafeGuard LAN Crypt\).

Kommandozeilensyntax:

```
SGLCInit <Startpfad | %Profile>[/S]
{-DIgnoreDirectory}[/Tv][/Te][/Tr][/Td]
[/Tdk {GUID}][/Dc][/De][/Dm][+FFiletype][/V1|/V2|/V3] [/X][/LLogfile]
```

Parameter:

- `Startpfad`
  Gibt entweder eine einzelne Datei an, die ver-, ent- oder umgeschlüsselt werden soll (z. B. C:\Daten\Vertrieb.doc), oder ein Verzeichnis, in dem die Ver-, Ent- oder Umschlüsselung durchgeführt werden soll (z. B. D:\Daten). Unterverzeichnisse werden standardmäßig nicht miteinbezogen!
- `%Profile`
  Arbeitet alle im geladenen Verschlüsselungsprofil enthaltenen Regeln mit absolutem Pfad ab. Ver-/entschlüsselt bzw. schlüsselt die Dateien wenn notwendig um.

Hinweis: Zum Entschlüsseln muss für die entsprechenden Dateien im Profil eine EXCLUDE Regel existieren.

- `/S`
  Inklusive aller Unterverzeichnisse ab dem Startpfad.
- `/h` oder `/?`
  Öffnet ein Hilfefenster zur Syntax von `sglcinit.exe`.
- -D*IgnoreDirectory*
  Ignoriere dieses Verzeichnis.
- `/Tv`
  Task Modus: v = Zeigt den Verschlüsselungsstatus der Dateien an.

- `/Te`
  Task Modus: e = Verschlüsselt wenn notwendig die Dateien entsprechend dem Verschlüsselungsprofil.
- `/Tr`
  Task Modus: r = Schlüsselt die Dateien wenn notwendig entsprechend dem Verschlüsselungsprofil um.
- `/Td`
  Task Modus: d = Entschlüsselt die Dateien wenn notwendig entsprechend dem Verschlüsselungsprofil.
- `/Tdk`
  Task Modus: dk = Entschlüsselt die Dateien, die mit den angegebenen Schlüsseln verschlüsselt sind. Es muss die GUID für die Schlüssel angegeben werden.

Hinweis: Alle Task Modus-Parameter können in einem Befehlsaufruf zusammen genutzt werden.

- `/Dc`
  Diese Option dekomprimiert NTFS komprimierte Dateien und verschlüsselt sie anschließend. Ist diese Option nicht gesetzt, werden NTFS komprimierte Dateien ignoriert.
- `/De`
  Diese Option entschlüsselt EFS verschlüsselte Dateien und verschlüsselt sie anschließend. Ist diese Option nicht ausgewählt, werden EFS verschlüsselte Dateien ignoriert.
- `/Dm`
  Diese Option entschlüsselt mehrfach verschlüsselte Dateien und verschlüsselt sie anschließend neu. Die Dateien sind dann wieder mit einem Schlüssel verschlüsselt.
- `+F`*Dateityp*
  Werden mit dieser Option Dateitypen angegeben (z. B. +Ftxt+Fdoc), werden ausschließlich Dateien vom angegebenen Typ bearbeitet. Diese Einstellung wirkt sich nur auf Dateien aus, für die eine Verschlüsselungsregel existiert.
  Befinden sich auch noch andere Dateien eines Typs, der nicht hier angegeben wird, in einem Verzeichnis, werden sie bei der Initialverschlüsselung nicht berücksichtigt. Sie werden erst verschlüsselt, wenn sie vom Benutzer geöffnet und wieder abgespeichert werden.
- `/V1`
  Verbose Modus 1: Nur Fehlermeldungen werden ausgegeben.
- `/V2`
  Verbose Modus 2: Ausgabe der Dateien, die ver/um/entschlüsselt werden sowie der Fehlermeldungen.

- `/V3`
  Verbose Modus 3: Ausgabe aller Dateien.
- `/E`
  Bei Fehler abbrechen.
- `/X`
  Initialverschlüsselung ohne Fenster ausführen.
- `/LLogfile`
  Ausgabe wird auch in die Datei geschrieben.

Hinweis: Der Parameter /Td kann nur dann mit %Profile sinnvoll kombiniert werden, wenn die zu entschlüsselnden Dateien im Profil über eine Exclude Regel aufgeführt sind. Andernfalls muss /Td mit Startpfad kombiniert werden.

Beispiel:

```
sglcinit.exe %PROFILE -DC:\ignorieren /S /Te /Tdk {1234ABCD-1234-1234-
1234-1234ABCD} {5678EFGH-5678-5678-5678-5678EFGH} /V1 /LC:\logfile.xml
```

5.5 Explorererweiterungen

Die SafeGuard LAN Crypt Explorererweiterungen bieten folgende Funktionalität:

- Initialverschlüsselung von Dateien und Verzeichnissen.
- Explizite Ver- und Entschlüsselung von Dateien und Verzeichnissen.
- Einfache Kontrolle über den Verschlüsselungsstatus Ihrer Daten.

SafeGuard LAN Crypt fügt dem Windows Explorer Einträge hinzu. Diese erscheinen in den Kontextmenüs von Laufwerken, Verzeichnissen und Dateien. Des Weiteren wird auch dem Windows Eigenschaften Fenster für Dateien ein Reiter mit Informationen zum *Verschlüsselungsstatus* hinzugefügt.

Bei einem Rechtsklick auf ein Verzeichnis oder eine Datei wird im Kontextmenü der Eintrag **SafeGuard LAN Crypt** angezeigt. Ist eine Datei ausgewählt, zeigt ein Schlüssel in verschiedenen Farben den Verschlüsselungsstatus der Datei an:

- **Grüner Schlüssel**
  Die Datei ist verschlüsselt, und der Benutzer hat Zugriff auf den Schlüssel.
- **Roter Schlüssel**
  Die Datei ist verschlüsselt, aber der Benutzer hat keinen Zugriff auf den Schlüssel.
- **Grauer Schlüssel**
  Die Datei ist unverschlüsselt, sollte aber an diesem Ort entsprechend einer vorhandenen Verschlüsselungsregel verschlüsselt sein.
- **Gelber Schlüssel**
  Die Datei ist verschlüsselt, die transparente Verschlüsselung ist aber derzeit deaktiviert.

Hinweis: Für Dateien, die das Offline-Attribut gesetzt haben (physikalisch nicht vorhanden), werden keine Schlüsselsymbole angezeigt.

Der Eintrag **SafeGuard LAN Crypt** des Kontextmenüs öffnet ein Untermenü, das weitere Einträge enthält. Diese Einträge können variieren, abhängig davon, ob ein Verzeichnis oder eine Datei ausgewählt wurde und in welchem Verschlüsselungszustand sich eine Datei befindet.

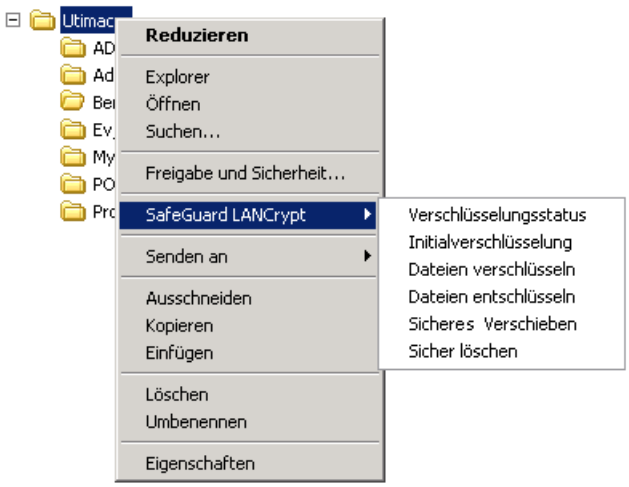
Hinweis: Auch den Ordnern und Dateien im Windows Explorer selbst werden Schlüsselsymbole hinzugefügt. Schlüssel in verschiedenen Farben zeigen den Verschlüsselungsstatus an:

- **Grüner Schlüssel**
  Die Datei ist verschlüsselt, und der Benutzer hat Zugriff auf den Schlüssel.
- **Roter Schlüssel**
  Die Datei ist verschlüsselt, aber der Benutzer hat keinen Zugriff auf den Schlüssel.

- **Grauer Schlüssel**
  Die Datei ist unverschlüsselt, sollte aber an diesem Ort entsprechend einer vorhandenen Verschlüsselungsregel verschlüsselt sein.

- **Gelber Schlüssel mit Fragezeichen**
  Der Benutzer verfügt nicht über die notwendigen Leserechte für die Datei. Daher kann SafeGuard LAN Crypt den Verschlüsselungsstatus nicht feststellen.

Folgende Einträge können in diesem Menü angezeigt werden:



Für Verzeichnisse:

- **Verschlüsselungsstatus**

  Klicken auf diesen Eintrag zeigt eine Liste aller Dateien in diesem Verzeichnis und ihren Verschlüsselungsstatus (farbige Schlüssel) an. Es werden immer nur die Dateien der ersten Verzeichnisebene angezeigt. Zur Anzeige der Dateien in Unterverzeichnissen muss auf das entsprechende Unterverzeichnis gewechselt werden. Im Explorer sind Verzeichnisse, für die eine Verschlüsselungsregel existiert, an einem Schlüsselsymbol zu erkennen.

- **Initialverschlüsselung**

  Verschlüsselt alle Dateien im Verzeichnis entsprechend dem geladenen Verschlüsselungsprofil. Auch Unterverzeichnisse, für die eine Verschlüsselungsregel gilt, werden miteinbezogen.
  Wie lange die Initialverschlüsselung ungefähr dauern wird, lässt sich an einem Fortschrittsbalken ablesen. Zudem wird angezeigt, wie viele Dateien das Verzeichnis insgesamt enthält und wie viele davon bereits verschlüsselt wurden. Dabei wird auch der Pfad zu der Datei angezeigt, die gerade verschlüsselt wird.

- **Dateien verschlüsseln**

  Verschlüsselt alle Dateien in der ersten Verzeichnisebene mit einem im geladenen Verschlüsselungsprofil vorhandenen Schlüssel. Es wird eine Liste der vorhandenen Schlüssel angezeigt, aus der jener Schlüssel, der zur Verschlüsselung aller Dateien verwendet werden soll, ausgewählt werden kann.

- **Dateien entschlüsseln**

  Entschlüsselt alle Dateien in der ersten Verzeichnisebene. Dazu müssen die entsprechenden Schlüssel im Verschlüsselungsprofil vorhanden sein. Sollte dies nicht der Fall sein, bleiben diese Dateien verschlüsselt.

- **Sicheres Verschieben**

  Beim Verschieben eines Ordners über SafeGuard LAN Crypt werden die Dateien entsprechend der geltenden Verschlüsselungsregeln bei Bedarf am neuen Speicherort ver-, ent- bzw. umgeschlüsselt. Die Quelldateien werden nach dem Verschieben sicher gelöscht.

- **Sicheres Löschen**

  Beim sicheren Löschen wird der Speicherort der Dateien mehrmals überschrieben. Die Dateien können über den Papierkorb nicht wiederhergestellt werden.

Für einzelne Dateien:

- **Verschlüsselungsstatus**

  Zeigt den Verschlüsselungsstatus der Datei an. Bei verschlüsselten Dateien listet eine Popup-Infobox den zugehörigen Schlüssel und gibt Auskunft, ob der Benutzer berechtigt ist, diesen Schlüssel zu verwenden. Ist ein anderer Benutzer angemeldet, der nicht berechtigt ist, erscheint in der Infobox anstelle des Schlüsselnamens die GUID.
  Verschlüsselte Dateien sind im Explorer an einem kleinen grünen Schlüsselsymbol zu erkennen.
  Über *Ordneroptionen/Ansicht/Erweiterte Einstellungen* kann der Benutzer für sein Profil festlegen, ob der Verschlüsselungsstatus von Dateien und der Status von Verschlüsselungsregeln auf Ordnern angezeigt wird oder nicht. Änderungen an diesen Einstellungen werden erst wirksam, nachdem sich der Benutzer ab- und wieder angemeldet hat.

- **Initialverschlüsselung**

  Verschlüsselt eine Datei entsprechend dem geladenen Verschlüsselungsprofil. Dieser Eintrag wird im Kontextmenü nur dann angezeigt, wenn der Verschlüsselungsstatus einer Datei nicht mit dem Verschlüsselungsprofil übereinstimmt.

- **Dateien verschlüsseln**

  Erlaubt die explizite Verschlüsselung einer Datei. Es wird eine Liste der verfügbaren Schlüssel angezeigt, aus welcher der entsprechende Schlüssel ausgewählt werden kann.

- **Dateien entschlüsseln**

  Entschlüsselt die ausgewählte Datei. Dazu muss der entsprechende Schlüssel im Verschlüsselungsprofil vorhanden sein. Sollte dies nicht der Fall sein, bleibt die Datei verschlüsselt.

- **Sicheres Verschieben**

  Beim Verschieben über SafeGuard LAN Crypt werden die Dateien entsprechend der geltenden Verschlüsselungsregeln bei Bedarf ver-, ent- bzw. umgeschlüsselt. Die Quelldateien werden nach dem Verschieben sicher gelöscht.

- **Sicheres Löschen**

  Beim sicheren Löschen wird der Speicherort der Dateien mehrmals überschrieben. Die Dateien können über den Papierkorb nicht wiederhergestellt werden.

Hinweis: Geladene Verschlüsselungsregeln haben immer Vorrang vor einer expliziten Verschlüsselung/Entschlüsselung mit den Befehlen **Dateien entschlüsseln/Dateien verschlüsseln**. Sollten Sie versuchen, Dateien zu ent-/verschlüsseln, für die eine Verschlüsselungsregel etwas anderes definiert, wird der Befehl nicht ausgeführt und es wird eine Fehlermeldung angezeigt. In folgenden Situationen kommt es beim Versuch, Dateien über das Kontextmenü zu verschlüsseln, zu einer Fehlermeldung:

- das Verzeichnis enthält Dateien, die mit einem unbekannten Schlüssel verschlüsselt sind.
- Wenn versucht wird, eine Datei im Widerspruch zu ihrer Verschlüsselungsregel zu ver-/entschlüsseln (z. B. wenn ein anderer Schlüssel gewählt wird, als in der Regel definiert, ...).

5.5.1 Verschlüsselungsinformation

Zusätzlich wird dem Standard-Eigenschaften Dialog von Windows ein Reiter mit Verschlüsselungsinformationen hinzugefügt. Dieser zeigt Informationen über die verschlüsselte Datei an.

5.6 Aktivieren und Deaktivieren der transparenten Verschlüsselung

Wenn die transparente Verschlüsselung im SafeGuard LAN Crypt Benutzermenü deaktiviert wird, hat dies zur Folge, dass die Dateien, auf die nach der Deaktivierung zugegriffen wird, nicht mehr automatisch ver- bzw. entschlüsselt werden. Neu erzeugte Dateien bleiben ebenfalls unverschlüsselt, auch wenn für diese eine Verschlüsselungsregel im Verschlüsselungsprofil des Benutzers vorhanden ist.

Hinweis: Die Deaktivierung der Verschlüsselung ist von Bedeutung, wenn verschlüsselte Dateien beim Kopieren/Verschieben in ein Verzeichnis, für das keine Verschlüsselungsregel besteht, verschlüsselt bleiben sollen oder wenn verschlüsselte Dateien an eine E-Mail angehängt werden sollen. Entsprechend der Philosophie von SafeGuard LAN Crypt würden diese Dateien entschlüsselt werden, wenn sie in ein unverschlüsseltes Verzeichnis kopiert oder als E-Mail Attachment versendet werden.

Wurde dagegen vom Administrator die Funktion *Persistente Verschlüsselung* aktiviert, bleiben Dateien automatisch auch dann verschlüsselt, wenn sie über den Windows Explorer in ein Verzeichnis verschoben werden, für das keine Verschlüsselungsregel existiert. Mit der persistenten Verschlüsselung ist es in den beschriebenen Fällen nicht mehr erforderlich, vorher die transparente Verschlüsselung zu deaktivieren. Die persistente Verschlüsselung sorgt dafür, dass Dateien auch dann verschlüsselt bleiben, wenn sie versehentlich in ein anderes Verzeichnis verschoben wurden oder wenn der Benutzer vergessen hat, die Verschlüsselung vor dem Verschieben bzw. Kopieren zu deaktivieren. Das Aktivieren oder Deaktivieren der persistenten Verschlüsselung wird erst nach einem Reboot des Client-Rechners wirksam.

Hinweis: Wenn ein Benutzer bei aktivierter persistenter Verschlüsselung eine Datei in ein Verzeichnis verschiebt oder kopiert, für das eine Ignorieren-Regel oder Ausnahmeregel gilt, erhält er einen Warnhinweis, dass die Datei dadurch entschlüsselt wird.

5.6.1 Transparente Verschlüsselung und Komprimierungsprogramme

Komprimierungsprogramme öffnen die Dateien, lesen den Inhalt und komprimieren ihn. Wenn die transparente Ent-/Verschlüsselung aktiviert ist, erhalten diese Programme die entschlüsselten Dateien und diese werden dann komprimiert. Die Dateien im Archiv sind nicht mehr verschlüsselt.

Wird das Archiv in einem Verzeichnis, für das keine Verschlüsselungsregel existiert, gespeichert, sind nun alle Dateien im Klartext gespeichert.

Auch wenn die persistente Verschlüsselung aktiviert ist, werden die Dateien nicht verschlüsselt komprimiert, da sich diese nur auf das Kopieren/Verschieben im Windows Explorer bezieht.

Um sicherzustellen, dass Dateien von Komprimierungsprogrammen verschlüsselt komprimiert werden, muss die transparente Verschlüsselung während der Verwendung solcher Programme deaktiviert werden.

Eine weitere Möglichkeit sicherzustellen, dass Dateien verschlüsselt komprimiert werden, besteht darin, Komprimierungsprogramme als *Unberücksichtigte Anwendung* zu definieren. Dies muss vom Security Officer vorgenommen werden.

5.7 Kompatibilität mit älteren Versionen

Bei einem gleichzeitigen Einsatz der neuen SafeGuard LAN Crypt 3.71 Software mit älteren Versionen sind folgende Punkte zu beachten:

- Der SafeGuard LAN Crypt 3.71 Client kann nur Profile laden, die mit der neuen Version 3.60 der SafeGuard LAN Crypt Administration erstellt wurden.
- Ältere SafeGuard LAN Crypt Clients können die mit Version 3.60 erstellten Profile und Regeln nutzen (abgesehen von Ausnahmen wie z. B. mit Unicode Japanisch erstellte Regeln, da diese Funktion erst ab 3.50 unterstützt wird).
- SafeGuard LAN Crypt Clients vor der Version 3.50 können Dateien, die mit der Version 3.50 oder höher verschlüsselt wurden, nicht lesen. Der neue Client lässt sich so konfigurieren, dass er für die Verschlüsselung von Dateien das alte Format verwendet
- Der SafeGuard LAN Crypt 3.71 Client dagegen kann auch Dateien lesen, die mit älteren Clients verschlüsselt wurden.

5.8 Deinstallation des Clients

Die Deinstallation des SafeGuard LAN Crypt Client erfolgt über die Systemsteuerung von Windows:
Wählen Sie unter Start/Einstellungen/Systemsteuerung/Software den Eintrag *SafeGuard LAN Crypt Client* und klicken Sie auf *Entfernen*.

In beiden Fällen ist anschließend ein Reboot erforderlich, damit die Änderungen wirksam werden.

Hinweis: Mit SafeGuard LAN Crypt verschlüsselte Dateien können nicht mehr entschlüsselt werden, wenn der SafeGuard LAN Crypt Client deinstalliert wurde.

5.9 Anhang: Fehlermeldungen beim Laden des Profils

Wenn beim Laden des Profils Probleme auftreten, weist der SafeGuard LAN Crypt Client den Benutzer durch folgende Fehlermeldungen auf die Ursache hin:

- Benutzerzertifikat nicht gefunden.
- LAN Crypt Security Officer Zertifikat nicht gefunden!
- Problem beim Laden der Zertifikate - Vorgang abgebrochen ...
- Fehler bei der Überprüfung des Benutzerzertifikats.
- Benutzerzertifikat abgelaufen oder noch nicht gültig.
- LAN Crypt Security Officer Zertifikat abgelaufen oder noch nicht gültig.

- Benutzerzertifikat wurde eingezogen.
- LAN Crypt Security Officer Zertifikat wurde widerrufen.
- Fehler bei der Überprüfung des LAN Crypt Security Officer Zertifikats.
- Userprofil "%s" kann nicht ins lokale Cache Verzeichnis "%s" kopiert werden!
- Fehler beim Laden des Key Management Keys.
- Diese Version der Richtliniendatei wird nicht unterstützt.
- Privaten Schlüssel für das Zertifikat nicht gefunden. Bitte stecken Sie den richtigen Token in den Leser und probieren Sie es erneut.
- Der Aussteller des Zertifikats konnte nicht gefunden oder überprüft werden.
- Die Stamm-Zertifizierungsstelle des Zertifikats konnte nicht gefunden oder überprüft werden.
- Der Widerrufstatus des Zertifikats ist unbekannt. CRL nicht gefunden oder abgelaufen.
- Das Benutzerzertifikat hat nicht die passenden Schlüsselverwendungserweiterungen.
- Das Benutzerzertifikat hat nicht unterstützte Erweiterungen.
- Das Benutzerzertifikat ist mit dem nicht unterstützten Microsoft Base Cryptographic Service Provider verknüpft.
- Die angegebene PIN ist möglicherweise falsch!
- Der Aussteller des LAN Crypt Security Officer Zertifikats konnte nicht gefunden oder überprüft werden.
- Die Stamm-Zertifizierungsstelle des LAN Crypt Security Officer Zertifikats konnte nicht gefunden oder überprüft werden.
- Der Widerrufstatus des LAN Crypt Security Officer Zertifikats ist unbekannt. CRL nicht gefunden oder abgelaufen.
- Das LAN Crypt Security Officer Zertifikat hat nicht die passenden Schlüsselverwendungs-Erweiterungen.
- Das LAN Crypt Security Officer Zertifikat hat nicht unterstützte Erweiterungen.
- Kann Richtliniendatei nicht dekomprimieren.
- Download der Richtliniendatei fehlgeschlagen.

6 Rechtlicher Hinweis

Copyright © 1996 - 2010 Sophos Group. Alle Rechte vorbehalten. SafeGuard ist ein eingetragenes Warenzeichen der Sophos Group.

Alle anderen erwähnten Produkt- und Unternehmensnamen sind Warenzeichen oder eingetragene Warenzeichen der jeweiligen Inhaber.

Diese Publikation darf weder elektronisch oder mechanisch reproduziert, elektronisch gespeichert oder übertragen, noch fotokopiert oder aufgenommen werden, es sei denn, Sie verfügen entweder über eine gültige Lizenz, gemäß der die Dokumentation in Übereinstimmung mit dem Lizenzvertrag reproduziert werden darf, oder Sie verfügen über eine schriftliche Genehmigung des Urheberrechtsinhabers.

Copyright-Informationen von Drittanbietern finden Sie in der Datei *3rd_Party_Software.rtf* in Ihrem Produktverzeichnis.

7 Technischer Support

Technischen Support zu Sophos Produkten können Sie wie folgt abrufen:

- Rufen Sie das SophosTalk-Forum unter http://community.sophos.com/ auf und suchen Sie nach Benutzern mit dem gleichen Problem.
- Durchsuchen Sie die Sophos Support-Knowledgebase unter http://www.sophos.de/support/.
- Laden Sie Dokumentation zu den Produkten unter http://www.sophos.de/support/docs/ herunter.
- Senden Sie eine E-Mail an den technischen Support support@sophos.de und geben Sie die Versionsnummer(n), Betriebssystem(e) und Patch Level Ihrer Sophos Software sowie ggf. den genauen Wortlaut von Fehlermeldungen an.